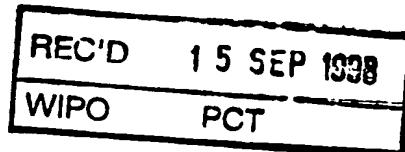


BUNDESREPUBLIK DEUTSCHLAND

09/446425

**PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)**Bescheinigung**

Die Siemens Aktiengesellschaft in München/Deutschland hat
eine Patentanmeldung unter der Bezeichnung

"Verfahren und Computersystem zur Codierung
einer digitalen Nachricht, zur Übertragung der
Nachricht von einer ersten Computereinheit zu
einer zweiten Computereinheit und zur Decodie-
rung der Nachricht"

am 26. Juni 1997 beim Deutschen Patentamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wie-
dergabe der ursprünglichen Unterlagen dieser Patentanmel-
dung.

Die Anmeldung hat im Deutschen Patentamt vorläufig die Sym-
bole H 04 L und G 06 F der Internationalen Patentklassifi-
kation erhalten.

München, den 14. Juli 1998

Der Präsident des Deutschen Patentamts

Im Auftrag

Aktenzeichen: 197 27 267.3

Agurks



This Page Blank (uspto)



1

Beschreibung

1. Bezeichnung

5 Verfahren und Computersystem zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht

10

2. Technischer Hintergrund

Es sind verschiedene Netzwerkprotokolle im Bereich des Managements von Rechnernetzen bekannt. Die Aufgaben für die Verwaltung von Rechnernetzen wird durch die hohe Verbreitung von 15 Computern und die immer komplexer werdende Vernetzung von Computern zunehmend schwieriger und die dafür erforderlichen Systeme zum Netzmanagement werden immer mächtiger. Im Rahmen der Verwaltung von Rechnernetzen gewinnt die Frage der Sicherheit des Netzmanagements immer größere Bedeutung. Die Sicherheit des Netzmanagements hängt sehr stark von den in dem 20 System verwendeten Sicherheitstechniken ab.

Aus dem Dokument (M. Rose, The Simple Book, PTR Prentice Hall, 2. Auflage, ISBN 0-13-177254-6, S. 59 - 91, 1994) sind verschiedene Netzwerkprotokolle für das Netzmanagement bekannt, beispielsweise das Simple-Network-Management-Protocol (SNMP) in der Version 1 (SNMPv1) und in der Version 2 (SNMPv2) oder auch das Common-Management-Internet-Protocol (CMIP).

30

Das SNMPv1 hat bisher die weiteste Verbreitung zur Überwachung und Kontrolle von Netzwerkkomponenten sowohl über lokale Rechnernetze (Local Area Networks, LANs), als auch bei globalen Netzen (Wide-Area-Networks, WANs).

35

Das SNMPv1 ist im Rahmen des OSI-Kommunikationsschichten-Systems oberhalb der Internetprotokolle User-Datagram-

Protocol (UDP) und Internet-Protocol (IP) angeordnet. Sowohl das UDP als auch das IP weisen erhebliche Schwächen im Bereich der Sicherheit auf, da Sicherheitsmechanismen in diesen Protokollen wenig bis gar nicht integriert sind.

5

Im weiteren werden sowohl das SNMP als auch CMIP als Netzwerkprotokoll bezeichnet.

Die Netzwerkprotokolle werden zur Übertragung von Rechner-
10 netz-Management-Information zwischen einer ersten Compu-
tereinheit, die einen sog. Manager enthält und mindestens ei-
ner zweiten Computereinheit, die einen sog. Agenten enthält,
verwendet. In einem komplexen Rechnernetz werden üblicherwei-
se mindestens eine Managementstation und eine beliebige An-
15 zahl von von der Managerapplikation überwachten und kontrol-
lierten Rechnern über das Netzwerkprotokoll überwacht bzw.
gesteuert.

Es sind jedoch ebenso Netzwerkmanagementarchitekturen be-
20 kannt, die mehrere Hierarchien aufweisen, beispielsweise meh-
rere Computer die von jeweils einem Manager überwacht werden,
und mehrere Computer, die jeweils eine Managerapplikation
enthalten, die wiederum von einem weiteren Computer, der eine
übergeordnete Managerapplikation enthält, überwacht bzw. kon-
25 trolliert werden.

Ein Computer, der eine Managerapplikation des jeweiligen
Netzwerkprotokolls enthält, wird im weiteren als erste Compu-
tereinheit bezeichnet.

30

Jede Computereinheit, die einen Agenten implementiert hat,
wird im weiteren als zweite Computereinheit bezeichnet.

35

Es ist möglich, daß ein Computer sowohl als Manager als auch
als Agent ausgestaltet ist, entsprechend sind die Funktional-
itäten in dem Computer enthalten.

Das jeweilige Netzwerkprotokoll kann in dem Computer sowohl in Hardware als auch in Software realisiert sein.

Im weiteren wird von einer einfachen Hierarchie ausgegangen,
5 d.h. es wird nur der Fall beschrieben, bei dem ein erster Computer als Manager eine beliebige Anzahl von zweiten Computern, die Agenten, überwacht, bzw. steuert. Dies dient jedoch lediglich der einfacheren Darstellung. Es ist ohne weiteres möglich, die Erfindung auch in einer Architektur mit einer
10 beliebigen Anzahl von Hierarchieebenen anzuwenden.

Bei den Netzwerkprotokollen wird von der ersten Computereinheit zu den zweiten Computereinheiten entweder eine Informationsabfrage übertragen oder es wird ein Steuerungswert zur
15 Steuerung bzw. Kontrolle der zweiten Computereinheit übertragen.

In jeder zweiten Computereinheit ist es bei den bekannten Netzwerkprotokollen üblich, daß die von der zweiten Computereinheit im Rahmen des Netzwerkprotokolls verwendete Information in Form einer sog. Management-Information-Base (MIB),
20 die die Struktur einer hierarchischen Datenbank aufweist, speichert.

Die Gesamtstruktur der Managementinformation der Netzwerkprotokolle wird in einem sog. globalen Registratur-Baum (Registration-Tree), beispielsweise dem globalen SNMP-Registration-Tree gespeichert. Die MIB eines Agenten, also einer zweiten Computereinheit, ist ein Teil des Registratur-Baums des jeweiligen Netzwerkprotokolls.
30

Zur Übertragung von Information zwischen der ersten Computereinheit und der zweiten Computereinheit werden digitale Nachrichten, beispielsweise eine SNMPv1-Nachricht verwendet.

35

Eine SNMPv1-Nachricht enthält eine Versionsnummer, einen sog. Community-String und eine SNMPv1-Protocol-Data-Unit (PDU).

Mit der Versionsnummer wird die Version des verwendeten Netzwerkprotokolls angegeben. Die Versionsnummer wird bei der Implementierung des jeweiligen Netzwerkprotokolls festgelegt.

5

Der Community-String bei der SNMPv1 dient als Passwort für den Zugang zu einer MIB einer zweiten Computereinheit. Der Community-String wird bei SNMPv1 unverschlüsselt zu dem Agenten gesendet. In dem Agenten, also der zweiten Computereinheit, wird überprüft, ob der Community-String, der jeweils zusammen mit einer SNMPv1-Nachricht empfangen wurde, zu einem Zugriff in der MIB der zweiten Computereinheit berechtigt. Da das Passwort bei SNMPv1 unverschlüsselt übertragen wird, ist ein Mißbrauch des Community-Strings leicht möglich, beispielsweise zur Maskierung eines potentiellen Angreifers und zum ungefugten Zugriff auf eine zweite Computereinheit, da es sehr einfach ist für einen potentiellen Angreifer, den Community-String zusammen mit einer IP-Senderadresse eines autorisierten Benutzers abzuhören.

20

SNMPv1 hat somit praktisch keinerlei wirkungsvolle Sicherheitsmechanismen integriert, insbesondere keine wirkungsvolle Authentifikation des SNMPv1-Managers und als Folge der fehlenden Authentifikation keine zuverlässige Zugriffskontrolle auf Seite des Agenten. Ferner enthält SNMPv1 keine Möglichkeit, Sicherheitsmechanismen der Datenintegrität oder der Datenvertraulichkeit zum implementieren. Somit ist es für einen potentiellen Angreifer ohne weiteres möglich, übertragene SNMP-PDUs einfach abzuhören und die übertragene Information zwischen Manager und Agent zu mißbrauchen.

Die Codierungsregeln der Netzwerkprotokolle sind detailliert in (M. Rose, The Simple Book, PTR Prentice Hall, 2. Auflage, ISBN 0-13-177254-6, S. 59 - 91, 1994) beschrieben.

35

Bei der zweiten Version des SNMP, dem SNMPv2 waren zwar verschiedene Sicherheitsmechanismen vorgesehen, jedoch war ins-

besondere die Verwaltung kryptographischer Schlüssel derart aufwendig, daß diese Problematik dazu führte, daß das SNMPv2 trotz erheblicher größerer Möglichkeiten zur Verwaltung von Rechnernetzen verglichen mit SNMPv1, sich gegenüber dem

5 SNMPv1 nicht auf dem Markt durchsetzen konnte. Daher wurde der ursprüngliche SNMPv2 Standard zurückgezogen und durch einen modifizierten Standard, bei dem keine Sicherheit integriert wurde, ersetzt.

10 Auch CMIP, das aufgrund allgemein wesentlich größerer Komplexität verglichen mit SNMPv1 und SNMPv2 kaum Berücksichtigung in Produkten gefunden hat, konnte sich auf dem Markt nicht durchsetzen.

15 Ferner ist das Konzept von sog. Proxy-Agenten ebenfalls in dem Dokument (M. Rose, The Simple Book, PTR Prentice Hall, 2. Auflage, ISBN 0-13-177254-6, S. 315, 1994) beschrieben.

3. Kurzbeschreibung der Erfindung

20 Somit liegt der Erfindung das Problem zugrunde, Verfahren sowie eine Computersysteme zur Codierung, Übertragung und Decodierung einer digitalen Nachricht anzugeben, bei der kryptographische Sicherheitsmechanismen vorgesehen sind, die einfacher sind als bei den bekannten Verfahren und Anordnungen.

Bei dem Verfahren gemäß Patentanspruch 1 wird eine digitale Nachricht, die von der ersten Computereinheit zu der zweiten Computereinheit übertragen werden soll, unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht codiert. Die codierte Nachricht wird mindestens einem kryptographischen Verfahren unterzogen und die kryptographisch bearbeitete codierte Nachricht wird wiederum unter Verwendung des Codierungsformats des Netzwerkprotokolls 30 codiert. Die codierte Nachricht wird wiederum unter Verwendung des Codierungsformats des Netzwerkprotokolls 35 codiert.

Bei dem Verfahren gemäß Patentanspruch 2 wird die Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls 5 codiert. Ferner wird die decodierte kryptographisch bearbeitete Nachricht einem zu dem mindestens einen kryptographischen Verfahren inversen kryptographischen Verfahren unterzogen und die invers kryptographisch bearbeitete Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls deco-10 diert.

Bei dem Verfahren gemäß Patentanspruch 3 wird eine digitale Nachricht, die von der ersten Computereinheit zu der zweiten Computereinheit übertragen werden soll, unter Verwendung ei-15 nes Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht codiert. Die codierte Nachricht wird mindestens einem kryptographischen Verfahren unterzogen und die kryptographisch bearbeitete codierte Nachricht wird wiederum unter Verwendung des Codierungsformats des Netzwerkprotokolls 20 codiert. Nach erfolgter Codierung wird die gesamte Nachricht von der ersten Computereinheit mindestens zur zweiten Computereinheit übertragen. Die empfangene Nachricht wird in der zweiten Computereinheit entsprechend dem Codierungsformat des Netzwerkprotokolls decodiert. Anschließend wird die decodier-25 te Nachricht dem zu dem verwendeten kryptographischen Verfahren inversen kryptographischen Verfahren unterzogen. In einem letzten Schritt wird die invers kryptographisch bearbeitete Nachricht entsprechend dem Codierungsformat des Netzwerkpro- tokolls decodiert.

30 Durch die "doppelte" Codierung bzw. Decodierung mit dem jeweiligen Netzwerkprotokoll wird eine sehr einfache, standard-konforme Lösung vorgeschlagen, die Übertragung von Nachrichten eines Netzwerkprotokolls kryptographisch abzusichern.

Das Verfahren weist ferner den erheblichen Vorteil der einfachen Realisierbarkeit und somit der schnellen Durchführbarkeit mit Hilfe eines Rechners auf.

5 Ein weiterer Vorteil ist darin zu sehen, daß die Netzwerkprotokolle unverändert bleiben können und keine neuen Netzwerkprotokolle definiert werden müssen. Somit ist keine aufwendige Versionsumstellung oder gar Neudefinition von Netzwerkprotokollen erforderlich. Die kryptographische Sicherheit des
10 jeweiligen Netzwerkprotokolls kann ohne größeren Aufwand erheblich erhöht werden.

Das Computersystem gemäß Patentanspruch 12 enthält mindestens
15 eine Recheneinheit, die derart eingerichtet ist, daß das Verfahren nach einem der Ansprüche 1 bis 11 durchgeführt wird.

Das Computersystem gemäß Patentanspruch 13 zur Codierung einer digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls, umfaßt mindestens folgende Komponenten:

- ein erstes Mittel zur Codierung der digitalen Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls zu einer codierten Nachricht,
- ein zweites Mittel zur kryptographischen Bearbeitung der codierten Nachricht,
- ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls.

30 Das Computersystem gemäß Patentanspruch 14 zur Decodierung einer digitalen Nachricht, welche in einem Codierungsformat eines Netzwerkprotokolls vorliegt, umfaßt mindestens folgende Komponenten:

35 -- ein fünftes Mittel zum Empfangen der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit,

- ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,
- ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht, und
- ein achtes Mittel zur Decodierung der invers kryptographisch bearbeiteten Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls.

10

Das Computersystem gemäß Patentanspruch 15 zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht enthält mindestens folgende Komponenten,

- eine erste Computereinheit, die mindestens folgende Komponenten umfaßt:
 - ein erstes Mittel zur Codierung der digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht,
 - ein zweites Mittel zur kryptographischen Bearbeitung der codierten Nachricht,
 - ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls,
 - ein viertes Mittel zum Senden der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit zu der zweiten Computereinheit,
- eine zweite Computereinheit, die mindestens folgende Komponenten umfaßt:
 - ein fünftes Mittel zum Empfangen der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit,
 - ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,

-- ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht, und

5 -- ein achtes Mittel zur Decodierung der invers kryptographisch bearbeiteten Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls.

Somit weisen die Computersysteme die oben im Zusammenhang mit dem Verfahren beschriebenen Vorteile ebenfalls auf.

10 Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

15 Besonders vorteilhaft ist das Verfahren im Zusammenhang mit SNMPv1 als Netzwerkprotokoll anwendbar, da für SNMPv1 bisher praktisch keine kryptographische Sicherheit vorhanden ist.

20 Doch auch bei den anderen Netzwerkprotokollen kann dieses Verfahren und die entsprechende Anordnung zur Durchführung des Verfahrens verwendet werden, da auch dort die Gesamtkomplexität des jeweiligen Netzwerkprotokolls erheblich reduziert wird.

Ferner ist es bei dem Computersystem vorteilhaft, ein zweites 30 Mittel zur kryptographischen Bearbeitung der codierten Nachricht, ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls sowie ein viertes Mittel zum Senden der codierten kryptographisch bearbeiteten Nachricht zu der zweiten Computereinheit als einen sog. Proxy-Agenten auszustalten, der über eine als gesichert angenommene Kommunikationsverbindung zu dem ersten Mittel zur Codierung der digitalen Nachricht unter Verwendung des Netzwerkprotokolls verbunden ist. Der erste Proxy-Agent und die erste Computereinheit 35 können gemeinsam in einer Computereinheit oder auch in zwei unterschiedlichen Computereinheiten realisiert sein.

Auf diese Weise wird unter Verwendung der Proxy-Technik, die aus dem Dokument (M. Rose, The Simple Book, PTR Prentice Hall, 2. Auflage, ISBN 0-13-177254-6, S. 315, 1994) bekannt ist, die Realisierung eines Computersystems zur kryptographisch sicheren Übertragung von Nachrichten des Codierungsformats eines Netzwerkprotokolls erreicht.

Dieser Vorteil ist ebenso dann gegeben, wenn ein fünftes Mittel zum Empfang der codierten kryptographisch bearbeiteten Nachricht, ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls sowie ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht zusammen in einem zweiten Proxy-Agenten realisiert sind, der über eine als gesichert angenommene Kommunikationsverbindung mit dem Agenten der zweiten Computereinheit unter Verwendung des Netzwerkprotokolls verbunden ist.

4. Kurzbeschreibung der Figuren

In den Fig. ist ein Ausführungsbeispiel der Erfindung dargestellt, die im weiteren näher erläutert wird.

Es zeigen

25 Fig. 1 ein Ablaufdiagramm, in dem das erfindungsgemäße Verfahren mit Realisierungsdetails für einen Get-Request dargestellt ist;

Fig. 2 ein Ablaufdiagramm, in dem das Verfahren in seinen Verfahrensschritten mit Realisierungsdetails für einen Set-Request dargestellt ist;

30 Fig. 3 ein Ablaufdiagramm, in dem das Verfahren in abstrakter Form dargestellt ist;

Fig. 4 eine Skizze eines möglichen Aufbaus einer kryptographisch bearbeiteten SNMPv1-Nachricht, in der der Sicherheitsmechanismus der Authentifikation der Originaldaten realisiert wird;

35 Fig. 5 der Aufbau einer möglichen kryptographisch bearbei-

11

teten SNMPv1-Nachricht, mit der die Sicherheitsdienste Integrität und Vertraulichkeit der übertragenen SNMPv1-Nachricht realisiert wird;

Fig. 6 5 der mögliche Aufbau einer kryptographisch bearbeiteten SNMPv1-Nachricht, in der der Sicherheitsdienst der Vertraulichkeit der SNMPv1-Nachricht realisiert wird;

5. Figurenbeschreibung

10

Get-Request

In Fig. 1 sind eine erste Computereinheit C1 und eine zweite Computereinheit C2 symbolhaft dargestellt. Die erste Computereinheit C1 weist eine Managerapplikation MA des SNMPv1 sowie einen ersten Proxy-Agenten PA1 auf.

15 Die zweite Computereinheit C2 weist einen SNMPv1-Agenten AG sowie einen zweiten Proxy-Agenten PA2 auf Seiten der zweiten 20 Computereinheit C2 auf.

In einem ersten Schritt 101 wird in der ersten Computereinheit C1 ein Get-Request gebildet. Unter der Bildung eines Get-Requests ist zu verstehen, daß eine digitale Nachricht unter Verwendung eines Codierungsformats des SNMPv1-Netzwerkprotokolls zu einer codierten Nachricht, dem Get-Request, codiert wird. Dies erfolgt in einem ersten Mittel 101 der ersten Computereinheit C1 zur Codierung der digitalen Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls.

30 In einem zweiten Schritt 102 wird der Get-Request, d.h. die codierte Nachricht CN von dem ersten Mittel M1 zu dem ersten Proxy-Agenten PA1 auf der Seite der ersten Computereinheit C1 gesendet.

In dem ersten Proxy-Agenten PA1 wird in einem dritten Schritt 103 die codierte Nachricht CN empfangen.

5 In einem vierten Schritt 104 wird die codierte Nachricht CN in dem ersten Proxy-Agenten PA1 mindestens einem kryptographischen Verfahren unterzogen. Zur kryptographischen Bearbeitung der codierten Nachricht in dem vierten Schritt 104 wird ein zweites Mittel 104 eingesetzt.

10 Unter einem kryptographischen Verfahren ist jedes beliebige kryptographische Verfahren z.B. zur Authentifikation, zur Sicherung der Datenintegrität oder auch zur Verschlüsselung von digitalen Daten zu verstehen. Hierbei können beispielsweise das RSA-Verfahren oder auch der Data-Encryption-Standard, der 15 als DES-Verfahren bezeichnet wird, Verwendung finden.

Als Ergebnis erhält man eine kryptographisch bearbeitete Nachricht KBN, deren Format beispielsweise in den Fig. 3 bis 6 dargestellt ist und im weiteren näher erläutert wird.

20

In einem fünften Schritt 105 wird die kryptographisch bearbeitete Nachricht KBN wiederum unter Verwendung des Codierungsformats des SNMP-Netzwerkprotokolls codiert. Unter diesem Verfahrensschritt ist zu verstehen, daß der kryptographisch bearbeitete Get-Request vorzugsweise in einem Set-Request codiert wird, d.h. eingekapselt wird. Ferner ist ein drittes Mittel 105 zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls vorgesehen.

30

Wie im weiteren deutlich wird, ist es vorteilhaft, jede Art von Nachricht, die von der ersten Computereinheit C1 zu der zweiten Computereinheit C2 übertragen werden soll, in dem fünften Schritt 105 als Set-Request zu codieren. Dies ist vorteilhaft, da die Syntax von SNMPv1 für einen Get-Request lediglich Object-Identifiers als zu übertragende Nutzdaten erlaubt. Es ist bei SNMPv1 nicht möglich, die kryptographisch

bearbeitete Information in einem SNMP-Get-Request einzubinden.

5 In einem sechsten Schritt 106 wird der Set-Request als codierte kryptographisch bearbeitete Nachricht CKN von der ersten Computereinheit C1 zu der zweiten Computereinheit C2, d.h. von dem ersten Proxy-Agenten PA1 zu einem zweiten Proxy-Agenten PA2 übertragen.

10 Von dem zweiten Proxy-Agenten PA2 der zweiten Computereinheit C2 wird die codierte kryptographisch bearbeitete Nachricht CKN in einem siebten Schritt 107 empfangen. Hierzu ist ein fünftes Mittel 107 zum Empfangen der codierten kryptographisch bearbeiteten Nachricht CKN vorgesehen.

15 In einem achtten Schritt 108 wird von dem zweiten Proxy-Agenten PA2 standardkonform eine Get-Response als Antwort auf den Set-Request an den ersten Proxy-Agenten PA1 der ersten Computereinheit C1 gesendet. Der Get-Response enthält als Bestätigung den jeweiligen Fehlerzustand.

20 In einem neunten Schritt 109 wird die empfangene codierte kryptographisch bearbeitete Nachricht CKN unter Verwendung des Codierungsformats des Netzwerkprotokolls entkapselt, d.h. decodiert. Es ist ein sechstes Mittel 109 zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des SNMPv1-Protokolls vorgesehen.

25 In einem zehnten Schritt 110 wird von dem zweiten Proxy-Agenten PA2 das zu dem jeweils vorgesehenen kryptographischen Verfahren inverse kryptographische Verfahren beispielsweise zur Authentifikation, zur Entschlüsselung bzw. zur Sicherung der Integrität der übertragenen Daten auf die decodierte kryptographisch bearbeitete Nachricht DKN angewendet. Hierzu ist ein siebtes Mittel 110 zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht DKN vorgesehen.

Weiterhin wird die invers kryptographisch bearbeitete Nachricht IKN, d.h. der originale Get-Request, von dem zweiten Proxy-Agenten PA2 zu der Agentenapplikation AG der zweiten 5 Computereinheit C2 gesendet.

In einem elften Schritt 111 wird der Get-Request von dem Agenten AG empfangen. Hierzu ist ein achtes Mittel 111 Empfangen des Get-Requests vorgesehen.

10

In einem weiteren Schritt 112 wird die invers kryptographisch bearbeitete Nachricht entsprechend dem Codierungsformat des SNMPv1-Protokolls zu der digitalen Nachricht decodiert, d.h. ausgewertet. Dies bedeutet, daß für den Spezialfall des Get- 15 Requests die über den Get-Request angeforderte Information eines Werts eines sog. Managed Objects (MO), der in der MIB des Agenten AG gespeichert ist, ausgelesen wird. Die Angabe, welche Information tatsächlich angefordert wird, ist als Object-Identifier in dem ursprünglichen Get-Request enthalten.

20

Es wird also in dem zwölften Schritt 112 die angeforderte Aktion ausgeführt, in diesem Fall das Auslesen der angeforderten Information, einen Wert eines Managed Objects. Hierzu ist ein neuntes Mittel 112 zur Durchführung der angeforderten Aktion 25 vorgesehen.

Wie es in SNMPv1 vorgesehen ist, wird von dem Agenten AG in der zweiten Computereinheit als Antwort auf einen Get-Request ein Get-Response gebildet und in einem dreizehnten Schritt 30 113 zu dem zweiten Proxy-Agenten PA2 gesendet. Der Get-Response erhält das Ergebnis der Aktion, die von der ersten Computereinheit C1 in dem Get-Request angefordert wurde.

Der Get-Response wird im weiteren als Antwortnachricht AN bezeichnet. Die Antwortnachricht AN kann entweder direkt zu der ersten Computereinheit C1 übertragen werden oder, zur weiteren Erhöhung der kryptographischen Sicherheit, entsprechend 35

dem Codierungsformat des Netzwerkprotokolls noch einmal codiert werden. Es ist in der zweiten Computereinheit C2 ein zehntes Mittel 112 zum Senden des Ergebnisses der Aktion zu der ersten Computereinheit C1 vorgesehen.

5

Weiterhin ist ein elftes Mittel 113 zur Bildung der Antwortnachricht AN vorgesehen, die das Ergebnis der Aktion enthält und zur Codierung der Antwortnachricht AN entsprechend dem Codierungsformat des SNMPv1-Protokolls.

10

In einem vierzehnten Verfahrensschritt 114 wird von dem zweiten Proxy-Agenten PA2 die Antwortnachricht AN empfangen. Hierzu ist ein zwölftes Mittel 114 zum Empfangen der Antwortnachricht AN vorgesehen.

15

In einem fünfzehnten Schritt 115 wird die codierte Antwortnachricht AN mindestens einem kryptographischen Verfahren unterzogen. Hierfür ist ein dreizehntes Mittel 115 zur Bearbeitung der Antwortnachricht AN mit mindestens einem kryptographischen Verfahren vorgesehen. Das Ergebnis dieses Verfahrensschritts ist eine in einem Sicherheitsrahmen eingekapselte Get-Response.

Die kryptographisch bearbeitete Antwortnachricht KBAN wird in einer Sicherheits-MIB in dem zweiten Proxy-Agenten PA2 gespeichert (Schritt 116). Der Aufbau der Sicherheits-MIB wird im weiteren detailliert beschrieben.

Um die kryptographisch bearbeitete Antwortnachricht KBAN zu erlangen, wird von dem ersten Proxy-Agenten PA1 der ersten Computereinheit C1 ein Get-Request, d.h. eine Abrufnachricht ABN gebildet. Hierfür ist ein vierzehntes Mittel 117 zur Bildung und Codierung der Abrufnachricht ABN entsprechend dem Codierungsformat des SNMPv1-Protokolls vorgesehen, mit der die kryptographisch bearbeitete Antwortnachricht KBAN von der zweiten Computereinheit C2 angefordert wird. Ferner wird die

codierte Abrufnachricht ABN von der ersten Computereinheit C1 zu der zweiten Computereinheit C2 gesendet.

5 In einem achtzehnten Schritt 118 wird in dem zweiten Proxy-Agenten PA2 die Abrufnachricht ABN, d.h. in diesem Fall der Get-Request, empfangen und standardkonform der übliche Get-Response, der in diesem Fall die kryptographisch bearbeitete Antwortnachricht KBAN enthält, an den ersten Proxy-Agenten PA1 gesendet. Hierzu ist in der zweiten Computereinheit C2 10 ein fünfzehntes Mittel 118 zum Empfangen der Abrufnachricht ABN und zur Codierung der in der Abrufnachricht ABN angeforderten kryptographisch bearbeiteten Antwortnachricht KBAN entsprechend dem Codierungsformat des SNMPv1-Protokolls, d.h. zur Codierung des angeforderten Get-Response vorgesehen.

15 15 Die codierte kryptographisch bearbeitete Antwortnachricht wird von dem zweiten Proxy-Agenten PA2 zu dem ersten Proxy-Agenten PA1 übertragen.

20 20 In einem weiteren Schritt 119 wird in dem ersten Proxy-Agenten PA1 die codierte kryptographisch bearbeitete Antwortnachricht, enthalten in der standardkonformen Get-Response, empfangen. Hierfür ist ein sechzehntes Mittel 119 zum Empfangen der Get-Response in der ersten Computereinheit C1 vorgesehen.

25 In einem weiteren Schritt 120 wird der Get-Request decodiert, d.h. entkapselt und der ursprünglich von dem Agenten AG der zweiten Computereinheit C2 gebildete Get-Response zu der Managerapplikation MA der ersten Computereinheit C1 gesendet. Hierfür ist ein siebzehntes Mittel 120 vorgesehen zum Decodieren der Get-Response und zum Senden der ursprünglichen, in der Get-Response enthaltenen Get-Response, die die angeforderte Information enthält, zu der Managerapplikation MA.

35 35 In einem letzten Schritt 121 wird die Get-Response von der Managerapplikation MA empfangen und der angeforderte Wert

ausgewertet und abgespeichert. Hierfür ist ein achtzehntes
Mittel 121 zum Empfangen und Auswerten von Managementinfor-
mation in der Managerapplikation MA vorgesehen.

5 Auf diese Weise wird erreicht, daß ohne großen Mehraufwand
und ohne das Verfahren des -SNMPv1-Protokolls ändert zu müs-
sen, eine kryptographische Sicherung der Kommunikation mög-
lich wird.

10 **Get-Next-Request**

Für einen Get-Next-Request, der ebenfalls im Rahmen des
SNMPv1-Protokolls vorgesehen ist, wird das Verfahren auf die
gleiche Weise, wie für den Get-Request beschrieben, durchge-
15 führt, lediglich mit einem veränderten, entsprechend angepaß-
ten Object-Identifier für den angeforderten Wert des jeweili-
gen Managed Objects.

Set-Request

20 In Fig. 2 ist das Verfahren für einen Set-Request als codier-
te digitale Nachricht CN dargestellt. Zur einfacheren Erläu-
terung wird lediglich das Verfahren im weiteren beschrieben,
die Mittel sind entsprechend ausgestaltet, daß die einzelnen
Verfahrensschritte mit den Computereinheiten C1, C2 durchge-
führt werden können.

In einem ersten Schritt 201 wird der Set-Request, d.h. die
digitale Nachricht codiert.

30 In einem zweiten Schritt 202 wird von dem Manager MA der er-
sten Computereinheit der Set-Request, d.h. die codierte Nach-
richt CN zu dem ersten Proxy-Agenten PA1 gesendet.

35 In einem dritten Schritt 203 wird die codierte Nachricht CN
von dem ersten Proxy-Agenten PA1 empfangen.

In einem vierten Schritt 204 wird ein kryptographisches Verfahren auf die codierte Nachricht CN angewendet. Das Ergebnis der kryptographischen Bearbeitung ist eine kryptographisch bearbeitete Nachricht KBN.

5

In einem fünften Schritt 205 wird die kryptographisch bearbeitete Nachricht KBN wiederum unter Verwendung des Codierungsformats des SNMPv1-Protokolls codiert zu einer codierten kryptographisch bearbeiteten Nachricht CKN. Hierfür wird wiederum ein Set-Request verwendet.

Der Set-Request wird von dem ersten Proxy-Agenten PA1 zu dem zweiten Proxy-Agenten PA2 gesendet (Schritt 206).

15 In einem siebten Schritt 207 wird von dem zweiten Proxy-Agenten PA2 der Set-Request empfangen.

Als Reaktion auf den Empfang des Set-Requests sendet standardkonform der zweite Proxy-Agent PA2 eine Get-Response, die 20 als Bestätigung den Fehlerzustand enthält (Schritt 208).

In einem weiteren Schritt 209 wird die codierte kryptographisch bearbeitete Nachricht decodiert, d.h. "ausgepackt". Das Ergebnis ist die decodierte kryptographisch bearbeitete Nachricht DKN.

25 In einem zehnten Schritt 210 wird jeweils das zu dem verwendeten kryptographischen Verfahren inverse kryptographische Verfahren auf die kryptographisch bearbeitete Nachricht DKN angewendet. Ferner wird die invers kryptographisch bearbeitete Nachricht IKN, d.h. der ursprüngliche Set-Request von dem zweiten Proxy-Agenten PA2 zu dem Agenten AG der zweiten Computerseinheit C2 gesendet.

35 In einem elften Schritt 211 wird von dem Agenten AG die decodierte kryptographisch bearbeitete Nachricht empfangen und in

einem weiteren Schritt 212 die in dem Set-Request angegebene Aktion durchgeführt.

5 Als Reaktion sendet der Agent AG der zweiten Computereinheit C2 standardkonform die Antwortnachricht AN in Form eines Get-Response zu dem zweiten Proxy-Agenten PA2 (Schritt 213).

In einem vierzehnten Schritt 214 empfängt der zweite Proxy-Agent PA2 die Antwortnachricht AN.

10 In einem fünfzehnten Schritt 215 wird wiederum auf die Antwortnachricht AN mindestens ein vorgebares kryptographisches Verfahren angewendet.

15 Die weiteren Verfahrensschritte 216, 217, 218, 219, 220 sowie 221 entsprechen den in Zusammenhang mit einem Get-Request beschriebenen Verfahren, den Verfahrensschritten 116, 117, 118, 119, 120 sowie 121.

20 Die Sicherheits-MIB enthält Einträge, die in ihrer Struktur die übliche Syntax zur Beschreibung von Managed-Objects verwendet. Einträge in der Sicherheits-MIB werden eindeutige Object-Identifiers zugeordnet, die zur eindeutigen Identifizierung der Einträge in der Sicherheits-MIB verwendet werden. Die Object-Identifiers werden in der globalen SNMP-MIB registriert. Damit wird erreicht, daß der Zweck und die Syntax des jeweiligen Managed-Objects bekannt ist. Die verschiedenen Einträge der Sicherheits-MIB können beispielsweise entweder digital unterzeichnete, integritätsgeschützte, oder verschlüsselte Managementinformation enthalten. Selbstverständlich können beliebige Kombinationen der oben beschriebenen Mechanismen in der Sicherheits-MIB eingetragen sein und somit im Rahmen des Verfahrens berücksichtigt werden.

35 Im weiteren wird eine mögliche Beispiel-Syntax in ASN.1 (Abstract Syntax Notation One) einer solchen Sicherheits-MIB dargestellt.

Die Syntax eines sicheren, eingekapselten Managed-Objects ist OCTET STRING. Der Aufbau eines solchen eingekapselten Managed-Objects ist wie folgt:

```
SecureMO ::=  
    SEQUENCE {  
        PlainHeader,  
        EncapsulatedData  
5    }  
  
PlainHeader ::=  
    SEQUENCE {  
        SecurityAssociationID,  
10       UsedAlgorithms,  
        AlgorithmParameters  
    }  
  
EncapsulatedData ::= OCTET STRING  
15       -- signed, encrypted, or integrity protected  
       -- ASN.1-encoded data  
  
SecurityAssociationID ::= OBJECT IDENTIFIER  
  
20 UsedAlgorithms ::= INTEGER (0..7)  
       -- value 0 stands for "no security"  
       -- value 1 stands for "signed"  
       -- value 2 stands for "integrity protected"  
       -- value 3 stands for "signed" and "integrity protected"  
       -- value 4 stands for "encrypted"  
       -- value 5 stands for "signed" and "encrypted"  
       -- value 6 stands for "integrity protected" and  
       --      "encrypted"  
       -- value 7 stands for "signed", "integrity protected"  
30       --      and "encrypted"  
  
AlgorithmParameters ::=  
       -- necessary parameters for the particular  
       -- algorithms in use
```

Der Wert des Parameters UsedAlgorithms wird nach dem folgenden Schema gebildet. Er kann als Bit-String der Länge 3 Bit repräsentiert werden, wobei das Bit niedrigster Wertigkeit die Verwendung digitaler Signatur („signed“) anzeigt, das Bit 5 mit zweitniedrigster Wertigkeit beispielsweise anzeigt, ob Mechanismen zur Sicherung der Datenintegrität vorgesehen sind („integrity protected“), und das Bit mit der höchsten Wertigkeit beschreibt, ob die Daten verschlüsselt wurden („encrypted“).

10

Somit kann das Ergebnis jeder kryptographischen Bearbeitung einer Nachricht als ein Bit-String mit der Länge 3 beschrieben werden. Die kryptographisch bearbeitete Nachricht wird als OCTET STRING codiert. Besteht sie aus einer nicht durch 8 15 teilbaren Anzahl von Bits, so kann sie jedoch durch Anwendung eines sog. Paddings, d.h. durch Auffüllen von Bits ohne semantische Bedeutung, zu einem OCTET STRING erweitert werden.

Diese Situation ist beispielhaft in einem Ablaufdiagramm in 20 Fig. 3 dargestellt.

Ein SNMPv1-Request SR wird gemäß den Vorschriften zur Codierung des jeweiligen Netzprotokolls in ASN.1 (Codierungsregeln, Syntaxdefinition, ER) codiert 301. Der codierte 25 SNMP-Request CSR, d.h. die codierte Nachricht CN wird in einem zweiten Schritt 302 dem jeweiligen kryptographischen Verfahren unterzogen. Hierbei werden beispielsweise kryptographische Schlüssel, Parameter zur Angabe des verwendeten Algorithmus, sowie zusätzliche Information, allgemein kryptographische Information VI, zur Durchführung des jeweiligen kryptographischen Verfahrens verwendet.

Der sich ergebende Bit-String BS wird beispielsweise durch 35 Auffüllen von Füllbits in einem Schritt 303 zu einem OCTET STRING OS konvertiert, z.B. unter Verwendung von Padding PA.

Die abstrakte Vorgehensweise zur inversen kryptographischen Bearbeitung wird entsprechend umgekehrt durchgeführt.

Es ist vorteilhaft, existierende Funktionen zur Sicherung der
5 Kommunikation im Rahmen von SNMPv1 dort anzuwenden, wo es möglich ist und diese Sicherheitsfunktionen mit weiteren kryptographischen Verfahren zu verstärken, wo es nötig ist.

So ist es vorteilhaft, das Konzept von Community-Strings in
10 SNMPv1 auch im Rahmen dieses Verfahrens zu verwenden. Im Rahmen des Konzepts einer Community werden Gruppen definiert und den einzelnen Gruppen Zugriffsrechte für die jeweiligen Mitglieder der Gruppe zugeordnet. Eine Community und die der Community zugeordneten Zugriffsrechte sind Teil einer Konfiguration eines SNMPv1-Agenten. Es ist vorteilhaft, jeweils
15 Communities mit spezifischen Sicherheitsmechanismen zu assoziieren. So ist es beispielsweise möglich, einer Community unterschiedliche kryptographische Algorithmen, kryptographische Schlüssel und entsprechende Parameter, die im Rahmen des
20 kryptographischen Verfahren jeweils verwendet werden, Mitgliedern der Community zuzuordnen.

Standardkonforme Object-Identifier werden vorzugsweise als Angaben verwendet, welche in kryptographischen Verfahren verwendet werden sollen.

Bei der Sicherheitskonfiguration wird vorzugsweise anstelle von kryptographischen Schlüsseln Object-Identifier auf gespeicherte kryptographische Schlüssel verwendet, die im weiteren als Schlüssel-Identifier bezeichnet werden. Durch diese
30 Vorgehensweise wird das jeweilige Schlüsselmaterial besser gesichert.

Weiterhin kann das jeweilige Schlüsselmaterial dadurch stärker geschützt werden, daß beispielsweise die Dateien, in denen die kryptographischen Schlüssel gehalten werden, verschlüsselt werden oder spezielle Hardwareeinheiten zum Schutz

der kryptographischen Schlüssel vorgesehen sind, beispielsweise Chipkarten.

5 Die jeweils zu verwendenden Realisierungsdetails ergeben sich aus der Sicherheitspolitik, die entsprechend der Anwendung stark variieren kann.

Authentifikation des Datenursprungs

10 Um den Sicherheitsdienst der Authentifikation der Ursprungsdaten zu erreichen kann beispielsweise folgende Information in der kryptographisch bearbeiteten Nachricht vorgesehen sein (vgl. Fig. 4).

15 Der SNMPv1-Request, d.h. die codierte Nachricht CN, wird durch die kryptographische Bearbeitung mit folgenden Header- bzw. Trailer-Informationen umkapselt, wodurch die kryptographisch bearbeitete Nachricht KBN entsteht.

20 Ein Authentifikations-Header AH enthält einen Schlüssel-Identifier KID, mit dem der jeweils zu verwendende kryptographische Schlüssel angegeben ist über einen Object-Identifier, einen Algorithm-Identifier AID, mit dem der jeweils zu verwendende kryptographische Algorithmus zur Authentifikation angegeben ist, Algorithmus-Parameter AP, mit denen angegeben wird, welche Parameter im Rahmen der Authentifikation verwendet werden, ein Zeitstempel TS sowie eine Zufallszahl RN.

25 Ferner ist als Trailerinformation TI eine digitale Signatur DS vorgesehen. Als Algorithmus zur Authentifikation kann beispielsweise das asymmetrische RSA-Verfahren eingesetzt werden.

Zugriffskontrolle für Managementinformation

35 Die SNMPv1-Zugriffskontrolle basiert auf zwei Mechanismen.

Erstens wird jedem Managed-Object in einer MIB ein Zugriffs-
kontrollwert zugeordnet, der einen der drei folgenden Werte
aufweist:

- Read-Only,
- 5 - Read-Write,
- Write-Only,
- Not-Accessable.

Zweitens wird jeder Community in dem SNMPv1-
10 Agentenkonfiguration ein sog. MIB-View zusammen mit den je-
weiligen Zugriffsrechten zugeordnet. Ein MIB-View enthält ei-
ne vorgebbare Anzahl von Object-Identifiern, die die jeweili-
gen Unterbäume oder sog. Blätter des SNMP-Registratur-Baums
bezeichnet.

15 Die jeweiligen Zugriffsrechte weisen einen der folgenden Wer-
te auf:

- Read Only,
- Write-Only,
- 20 - Read-Write,
- None.

Sicherung der Datenintegrität eines SNMP-Requests

Zur Sicherung der Datenintegrität wird ein Mechanismus zur
kryptographischen Sicherung der Datenintegrität eingesetzt.
Hierfür werden Datenintegritätsprüfsummen über den gesamten
SNMPv1-Request oder einen Teil davon gebildet. Dies kann bei-
spielsweise mittels des DES im sog. Cipher-Block-Chaining-
30 Mode (CBC-Modus) erfolgen. Für diesen speziellen Mechanismus
ist die Verwendung eines 64 Bit langen Initialisierungswerts
erforderlich, der jeder Partei der jeweiligen Sicherheits-
gruppe bekannt sein muß. Der Initialisierungswert ist Teil
der Algorithmusparameter AP, die in der Header-Information HI
35 der kryptographisch bearbeiteten Nachricht KBN verwendet wird
(vgl. Fig. 5). Ferner weist die Header-Information HI einen
Schlüssel-Identifier KID sowie einen Algorithmus-Identifier

AID auf, deren Funktionalität gleich ist wie bei der Authentifikation.

5 Ferner ist in einer Trailer-Information TI ein Integritätsprüfwert ICV vorgesehen.

Verschlüsselung von SNMPv1-Requests

10 Vertraulichkeit der übertragenen SNMPv1-Daten kann auf ähnliche Weise erfolgen, wie die Sicherung der Datenintegrität. Zur Verschlüsselung kann beispielsweise wiederum das DES-Verfahren im CBC-Modus verwendet werden. In diesem Fall ist wiederum ein Initialisierungswert als Algorithmusparameter AP und einer Header-Information HI der kryptographisch bearbeiteten Nachricht KBN erforderlich (vgl. Fig. 6).

20 Wiederum ist in der Header-Information HI ein Schlüssel-Identifier KID sowie ein Algorithmus-Identifier AID mit oben beschriebener Funktionalität vorgesehen.

Weiterhin können Mechanismen zur Protokollierung der Kommunikation sowie zur Alarmgebung bei Auffinden von Angriffsversuchen vorgesehen sein.

25 Das Verfahren und das Computersystem können sehr vorteilhaft im Rahmen eines Szenarios verwendet werden, bei dem ein Anbieter eines Kommunikationsnetzes Bandbreite des Kommunikationsnetzes einem Dienstanbieter zur Verfügung stellt, der Dritten zusätzliche Dienste zur Verfügung stellt, die das
30 Kommunikationsnetz als solche nicht vorsieht. In diesem Zusammenhang kann das Verfahren sowie das Computersystem vorteilhaft beispielsweise zur Kontrolle oder auch zur Abrechnung der von dem Anbieter des gesamten Kommunikationsnetzes zur Verfügung gestellten Ressourcen dienen. In diesem Fall
35 wird der Manager auf einem Computer des Anbieters des gesamten Kommunikationsnetzes realisiert sein und ein Agent jeweils bei dem Anbieter zusätzlicher Dienste.

In einer Variante des oben beschriebenen Ausführungsbeispiels ist es vorgesehen, die Antwortnachricht direkt, ohne Warten auf eine Abrufnachricht, zu codieren und an die erste Computereinheit zu senden. Somit sind folgende Schritte in der zweiten Computereinheit nicht erforderlich:

- die Codierung einer Abrufnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls in der ersten Computereinheit, mit der die kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit angefordert wird,
- die Übertragung der Abrufnachricht von der ersten Computereinheit zu der zweiten Computereinheit, sowie
- das Empfangen der Abrufnachricht.

15 Entsprechendes gilt für das Computersystem.

Anschaulich kann das Verfahren derart beschrieben werden, daß zu dem standardkonformen Netzwerkprotokoll z.B. dem SNMPv1-Protokoll auf den jeweiligen SNMP-Request oder auch CMIP-Request, ein kryptographisches Verfahren angewendet wird, mit dem eine kryptographische Sicherung des SNMP-Requests bzw. dem CMIP-Request erreicht wird. Um jedoch die Verwendung standardkonformer SNMP-Verfahren zu ermöglichen, wird die kryptographisch bearbeitete Nachricht wiederum mit dem jeweiligen Codierungsformat des Netzwerkprotokolls codiert. Dies entspricht einer "doppelten" Anwendung des jeweiligen Netzwerkprotokolls auf die zu codierende Nachricht.

Patentansprüche

1. Verfahren zur Codierung einer digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls,

5 - bei dem die Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls zu einer codierten Nachricht codiert wird,

- bei dem die codierte Nachricht mindestens einem kryptographischen Verfahren unterzogen wird, und

10 - bei dem die kryptographisch bearbeitete Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls codiert wird.

2. Verfahren zur Decodierung einer digitalen Nachricht, welche in einem Codierungsformat eines Netzwerkprotokolls vorliegt,

- bei dem die Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls decodiert wird,

- bei dem die decodierte kryptographisch bearbeitete Nach-

20 rricht einem zu dem mindestens einen kryptographischen Verfahren inversen kryptographischen Verfahren unterzogen wird, und

- bei dem die invers kryptographisch bearbeitete Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls de- codiert wird.

25

3. Verfahren zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht,

30 - bei dem in der ersten Computereinheit folgende Schritte durchgeführt werden:

-- die Nachricht wird unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht codiert,

35 -- die codierte Nachricht wird mindestens einem kryptographischen Verfahren wird,

- die kryptographisch bearbeitete Nachricht wird unter Verwendung des Codierungsformats des Netzwerkprotokolls codiert,
- bei dem die codierte kryptographisch bearbeitete Nachricht von der ersten Computereinheit zu der zweiten Computereinheit übertragen wird,
- 5 - bei dem in der zweiten Computereinheit folgende Schritte durchgeführt werden:
 - die empfangene Nachricht wird entsprechend dem Codierungsformat des Netzwerkprotokolls decodiert,
 - 10 - die decodierte kryptographisch bearbeitete Nachricht wird einem zu dem mindestens einem kryptographischen Verfahren inversen kryptographischen Verfahren unterzogen, und
 - die invers kryptographisch bearbeitete Nachricht wird entsprechend dem Codierungsformat des Netzwerkprotokolls zu der 15 digitalen Nachricht decodiert.

- 4. Verfahren nach Anspruch 3,
 - bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
 - 20 - bei dem in der zweiten Computereinheit die angeforderte Aktion ausgeführt wird, und
 - bei dem in der zweiten Computereinheit das Ergebnis der Aktion in einer Antwortnachricht zu der ersten Computereinheit gesendet wird.

- 5. Verfahren nach Anspruch 3,
 - bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
 - bei dem in der zweiten Computereinheit die angeforderte Aktion ausgeführt wird,
 - 30 - bei dem in der zweiten Computereinheit eine Antwortnachricht gebildet wird, die ein Ergebnis der Aktion enthält,
 - bei dem in der zweiten Computereinheit die Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird,
 - 35 - bei dem in der zweiten Computereinheit die Antwortnachricht mindestens einem kryptographischen Verfahren unterzogen wird,

- bei dem in der zweiten Computereinheit die kryptographisch bearbeitete Antwortnachricht gespeichert wird,
- bei dem in der ersten Computereinheit eine Abrufnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird, mit der die kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit angefordert wird,
- 5 - bei dem die Abrufnachricht von der ersten Computereinheit zu der zweiten Computereinheit übertragen wird,
- bei dem die Abrufnachricht von der zweiten Computereinheit empfangen wird,
- 10 - bei dem die kryptographisch bearbeitete Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird, und
- bei dem die codierte kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit zu der ersten Computereinheit übertragen wird.

6. Verfahren nach Anspruch 3,

- bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
- 20 - bei dem in der zweiten Computereinheit die angeforderte Aktion ausgeführt wird,
- bei dem in der zweiten Computereinheit eine Antwortnachricht gebildet wird, die ein Ergebnis der Aktion enthält,
- 25 - bei dem in der zweiten Computereinheit die Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird,
- bei dem in der zweiten Computereinheit die Antwortnachricht mindestens einem kryptographischen Verfahren unterzogen wird,
- 30 - bei dem die kryptographisch bearbeitete Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls codiert wird, und
- bei dem die codierte kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit zu der ersten Computereinheit übertragen wird.

7. Verfahren nach einem der Ansprüche 2 bis 6,

bei dem in der zweiten Computereinheit die kryptographisch bearbeitete Antwortnachricht in einer Management Information Base (MIB) gespeichert wird.

- 5 8. Verfahren nach einem der Ansprüche 1 bis 4, bei dem als Netzwerkprotokoll das Simple Network Management Protocol Version 1 (SNMPv1) verwendet wird.
9. Verfahren nach Anspruch 8,
- 10 - bei dem in der ersten Computereinheit bei der Codierung der kryptographisch bearbeiteten Nachricht ein Set-Request gebildet wird, und - bei dem der Set-Request von der ersten Computereinheit zu der zweiten Computereinheit übertragen wird.
- 15 10. Verfahren nach Anspruch 8 oder 9, - bei dem als Abrufnachricht ein Get-Request verwendet wird, - bei dem bei der Codierung der angeforderten kryptographisch bearbeiteten Antwortnachricht ein Get-Response gebildet wird.
- 20 11. Verfahren nach einem der Ansprüche 4 bis 10, bei dem als Aktion eine Informationsabfrage und/oder eine Informationsangabe der zweiten Computereinheit übertragen wird.
12. Vorrichtung mit mindestens einer Recheneinheit, die derart eingerichtet ist, daß das Verfahren nach einem der Ansprüche 1 bis 11 durchführbar ist.
13. Vorrichtung zur Codierung einer digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls, das mindestens folgende Komponenten umfaßt:
 - ein erstes Mittel zur Codierung der digitalen Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls zu einer codierten Nachricht,
 - 35 - ein zweites Mittel zur kryptographischen Bearbeitung der codierten Nachricht,

- ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls.
- 5 14. Vorrichtung zur Decodierung einer digitalen Nachricht, welches in einem Codierungsformat eines Netzwerkprotokolls vorliegt, das mindestens folgende Komponenten umfaßt:
 - ein fünftes Mittel zum Empfangen der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit,
 - 10 -- ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,
 - ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht, und
 - 15 -- ein achtes Mittel zur Decodierung der invers kryptographisch bearbeiteten Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls.
- 20 15. Vorrichtung zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht,
 - bei dem eine erste Computereinheit vorgesehen ist, die mindestens folgende Komponenten umfaßt:
 - ein erstes Mittel zur Codierung der digitalen Nachricht unter Verwendung eines Codierungsformats eines Netzwerkprotokolls zu einer codierten Nachricht,
 - ein zweites Mittel zur kryptographischen Bearbeitung der codierten Nachricht,
 - ein drittes Mittel zur Codierung der kryptographisch bearbeiteten Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls,
 - ein viertes Mittel zum Senden der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit zu der zweiten Computereinheit,

- bei dem eine zweite Computereinheit vorgesehen ist, die mindestens folgende Komponenten umfaßt:
 - ein fünftes Mittel zum Empfangen der codierten kryptographisch bearbeiteten Nachricht von der ersten Computereinheit,
 - 5 -- ein sechstes Mittel zur Decodierung der empfangenen Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,
 - ein siebtes Mittel zur inversen kryptographischen Bearbeitung der decodierten kryptographisch bearbeiteten Nachricht,
 - 10 und
 - ein achtes Mittel zur Decodierung der invers kryptographisch bearbeiteten Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls.
- 15 16. Vorrichtung nach Anspruch 13 oder 15, bei dem als drittes Mittel das erste Mittel vorgesehen ist.
- 17. Vorrichtung nach Anspruch 14 oder 15, bei dem als achtes Mittel das sechste Mittel vorgesehen ist.
- 20 18. Vorrichtung nach einem der Ansprüche 15 bis 17,
 - bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
 - bei dem in der zweiten Computereinheit ein neuntes Mittel zur Durchführung der angeforderten Aktion vorgesehen ist, und
 - bei dem in der zweiten Computereinheit ein zehntes Mittel zum Senden des Ergebnisses der Aktion zu der ersten Computereinheit vorgesehen ist.
- 30 19. Vorrichtung nach einem der Ansprüche 15 bis 18,
 - bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
 - bei dem in der zweiten Computereinheit ein neuntes Mittel zur Durchführung der angeforderten Aktion vorgesehen ist,
 - 35 - bei dem in der zweiten Computereinheit ein elftes Mittel zur Bildung einer Antwortnachricht, die ein Ergebnis der Aktion enthält, vorgesehen ist,

- bei dem in der zweiten Computereinheit ein zwölftes Mittel zur Codierung Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,
- bei dem in der zweiten Computereinheit ein dreizehntes Mittel zur Bearbeitung der Antwortnachricht mit mindestens einem kryptographischen Verfahren vorgesehen ist,
- bei dem in der zweiten Computereinheit ein vierzehntes Mittel zur Speicherung der kryptographisch bearbeiteten Antwortnachricht vorgesehen ist,
- 5 10 - bei dem in der ersten Computereinheit ein fünfzehntes Mittel zur Bildung und Codierung einer Abrufnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls, mit der die kryptographisch bearbeitete Antwortnachricht von der zweiten Computereinheit angefordert wird, vorgesehen ist,
- 15 - bei dem in der ersten Computereinheit ein sechzehntes Mittel zum Senden der Abrufnachricht von der ersten Computereinheit zu der zweiten Computereinheit, vorgesehen ist,
- bei dem in der zweiten Computereinheit ein siebzehntes Mittel zum Empfangen der Abrufnachricht vorgesehen ist
- 20 - bei dem in der zweiten Computereinheit ein achtzehntes Mittel zur Codierung der in der Abrufnachricht angeforderten kryptographisch bearbeiteten Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls, vorgesehen ist, und
- 25 - bei dem in der zweiten Computereinheit ein neunzehntes Mittel zum Senden der codierten kryptographisch bearbeiteten Antwortnachricht von der zweiten Computereinheit zu der ersten Computereinheit, vorgesehen ist.
- 30 20. Vorrichtung nach einem der Ansprüche 15 bis 18,
 - bei dem die digitale Nachricht eine Anfrage zur Ausführung einer vorgebbaren Aktion enthält,
 - bei dem in der zweiten Computereinheit ein neuntes Mittel zur Durchführung der angeforderten Aktion vorgesehen ist,
 - bei dem in der zweiten Computereinheit ein elftes Mittel zur Bildung einer Antwortnachricht, die ein Ergebnis der Aktion enthält, vorgesehen ist,

- bei dem in der zweiten Computereinheit ein zwölftes Mittel zur Codierung Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls,
- bei dem in der zweiten Computereinheit ein dreizehntes Mittel zur Bearbeitung der Antwortnachricht mit mindestens einem kryptographischen Verfahren vorgesehen ist,
- bei dem in der zweiten Computereinheit ein achtzehntes Mittel zur Codierung der kryptographisch bearbeiteten Antwortnachricht entsprechend dem Codierungsformat des Netzwerkprotokolls, vorgesehen ist, und
- bei dem in der zweiten Computereinheit ein neunzehntes Mittel zum Senden der codierten kryptographisch bearbeiteten Antwortnachricht von der zweiten Computereinheit zu der ersten Computereinheit, vorgesehen ist.

15

- 21. Vorrichtung nach Anspruch 19 oder 20, bei dem das vierzehnte Mittel derart ausgestaltet ist, daß die kryptographisch bearbeitete Antwortnachricht in einer Management Information Base (MIB) gespeichert wird.

20

- 22. Vorrichtung nach einem der Ansprüche 13 bis 21, das derart ausgestaltet ist, daß als Netzwerkprotokoll das Simple Network Management Protocol Version 1 (SNMPv1) verwendet wird.

25

- 23. Vorrichtung nach Anspruch 13 oder 15,
 - das derart ausgestaltet ist, daß als Netzwerkprotokoll das Simple Network Management Protocol Version 1 (SNMPv1) verwendet wird, und
- bei dem das dritte Mittel zur Codierung der kryptographisch bearbeiteten Nachricht derart ausgestaltet ist, daß bei der Codierung der kryptographisch bearbeiteten Nachricht ein Set-Request gebildet wird.

35

- 24. Vorrichtung nach Anspruch 22,

- bei dem das fünfzehnte Mittel zur Bildung und Codierung der Abrufnachricht derart ausgestaltet ist, daß ein Get-Request gebildet wird,
- bei dem das achtzehnte Mittel zur Codierung der in der Abrufnachricht angeforderten kryptographisch bearbeiteten Antwortnachricht derart ausgestaltet ist, daß ein Get-Response gebildet wird.

5

25. Vorrichtung nach einem der Ansprüche 15 bis 24,
10 bei dem als Aktion eine Informationsabfrage und/oder eine Informationsangabe der zweiten Computereinheit vorgesehen ist.

26. Vorrichtung nach einem der Ansprüche 12 bis 25,
15 bei dem das zweite Mittel, das dritte Mittel und das vierte Mittel zusammen als ein erster Proxy Agent ausgestaltet sind, und/oder
bei dem das fünfte Mittel, das sechste Mittel und das siebte Mittel zusammen als ein zweiter Proxy Agent ausgestaltet sind.

20

27. Kommunikationssystem mit einem Managers eines Kommunikationsnetzes und eines Zwischenmanagers eines Kommunikationsnetzes, der das Kommunikationsnetz verwendet und weitere Dienste, die über die von dem Kommunikationsnetz angebotenen Dienste hinausgehen, Kunden anbietet mit einem Computersystem nach einem der Ansprüche 13 bis 26.

25

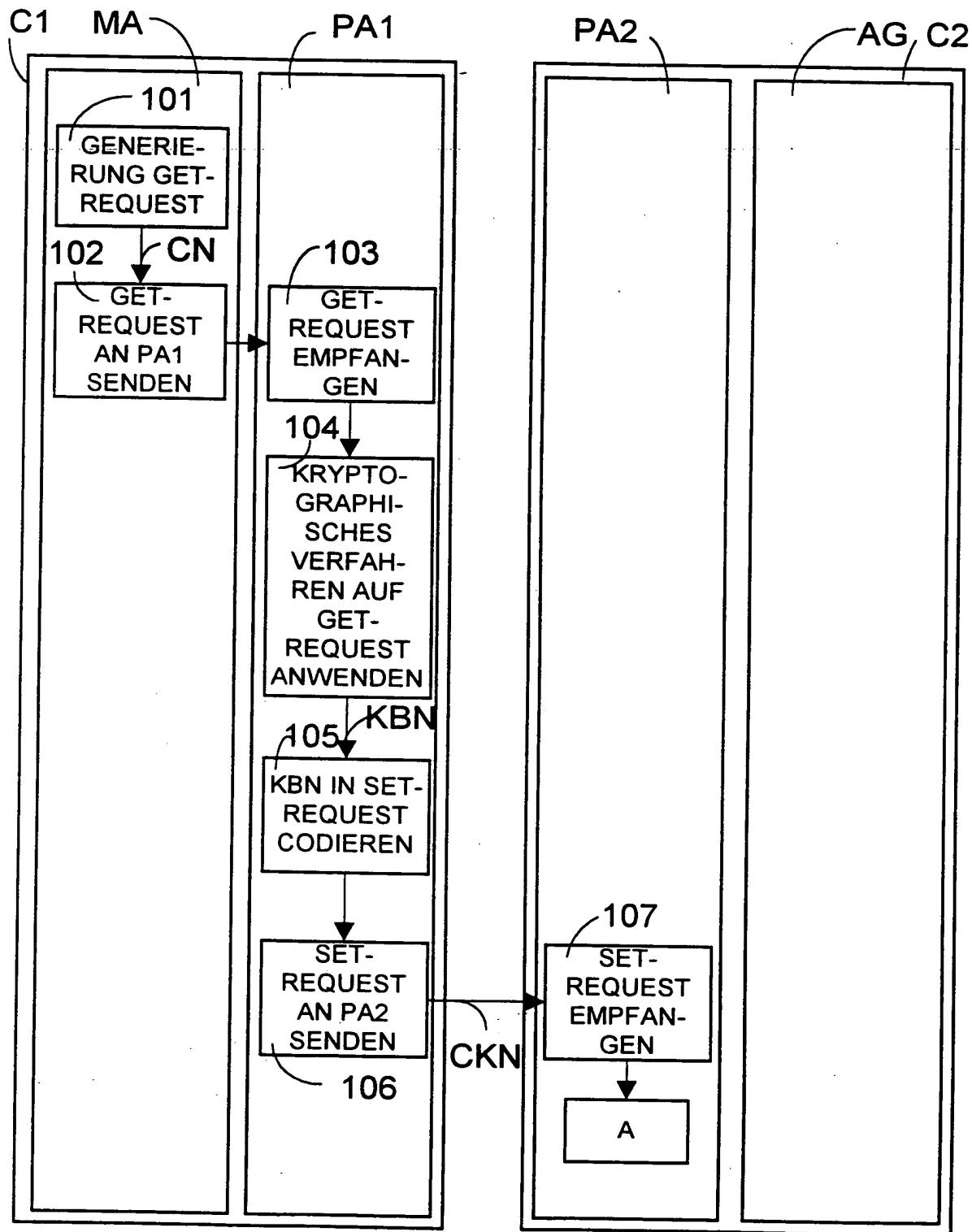
Zusammenfassung

Verfahren und Computersystem zur Codierung einer digitalen Nachricht, zur Übertragung der Nachricht von einer ersten 5 Computereinheit zu einer zweiten Computereinheit und zur Decodierung der Nachricht

Es wird ein Verfahren vorgestellt, bei dem für ein Netzwerk-protokoll, z.B. für das SNMPv1, wird in der ersten Computereinheit (C1) eine Nachricht unter Verwendung des Codierungsformats des Netzwerkprotokolls zu einer codierten Nachricht (CN) codiert (101). Die codierte Nachricht (CN) wird 10 einem kryptographischen Verfahren unterzogen (104). Die dadurch gebildete kryptographisch bearbeitete Nachricht (KBN) wird 15 wiederum unter Verwendung des Codierungsformats des Netzwerkprotokolls codiert (105). Die auf diese Weise codierte kryptographisch bearbeitete Nachricht (CKN) wird von der erste Computereinheit (C1) zu der zweiten Computereinheit 20 (C2) übertragen. In der zweiten Computereinheit (C2) wird die empfangene Nachricht entsprechend dem Codierungsformat des Netzwerkprotokolls decodiert (109) und es wird ein inverses kryptographisches Verfahren (110) auf die decodierte Nachricht (DKN) angewendet. Die invers kryptographisch bearbeitete Nachricht (IKN) wird entsprechend dem Codierungsformat des Netzwerkprotokolls wiederum decodiert.

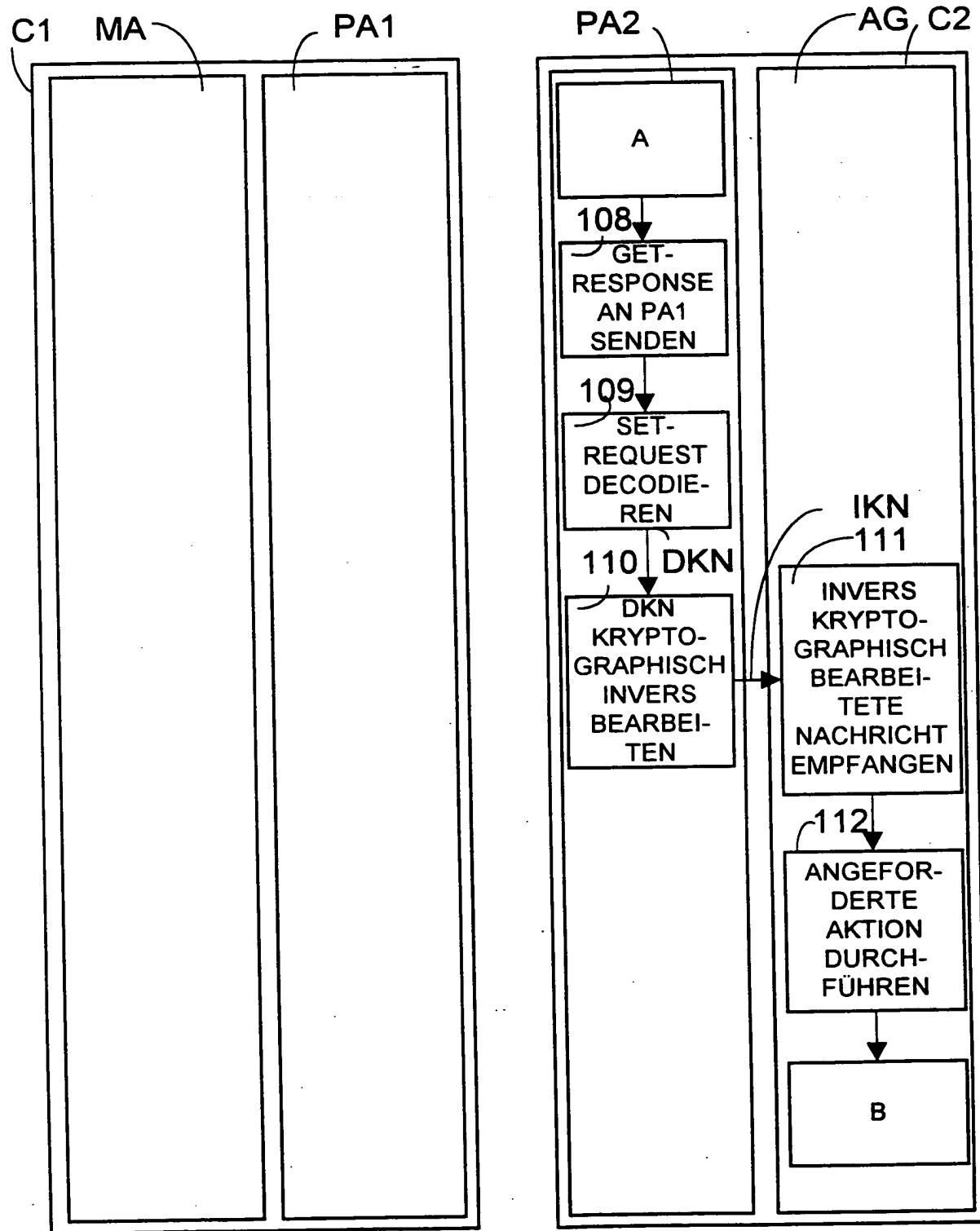
Sig. Fig. 1

FIG 1



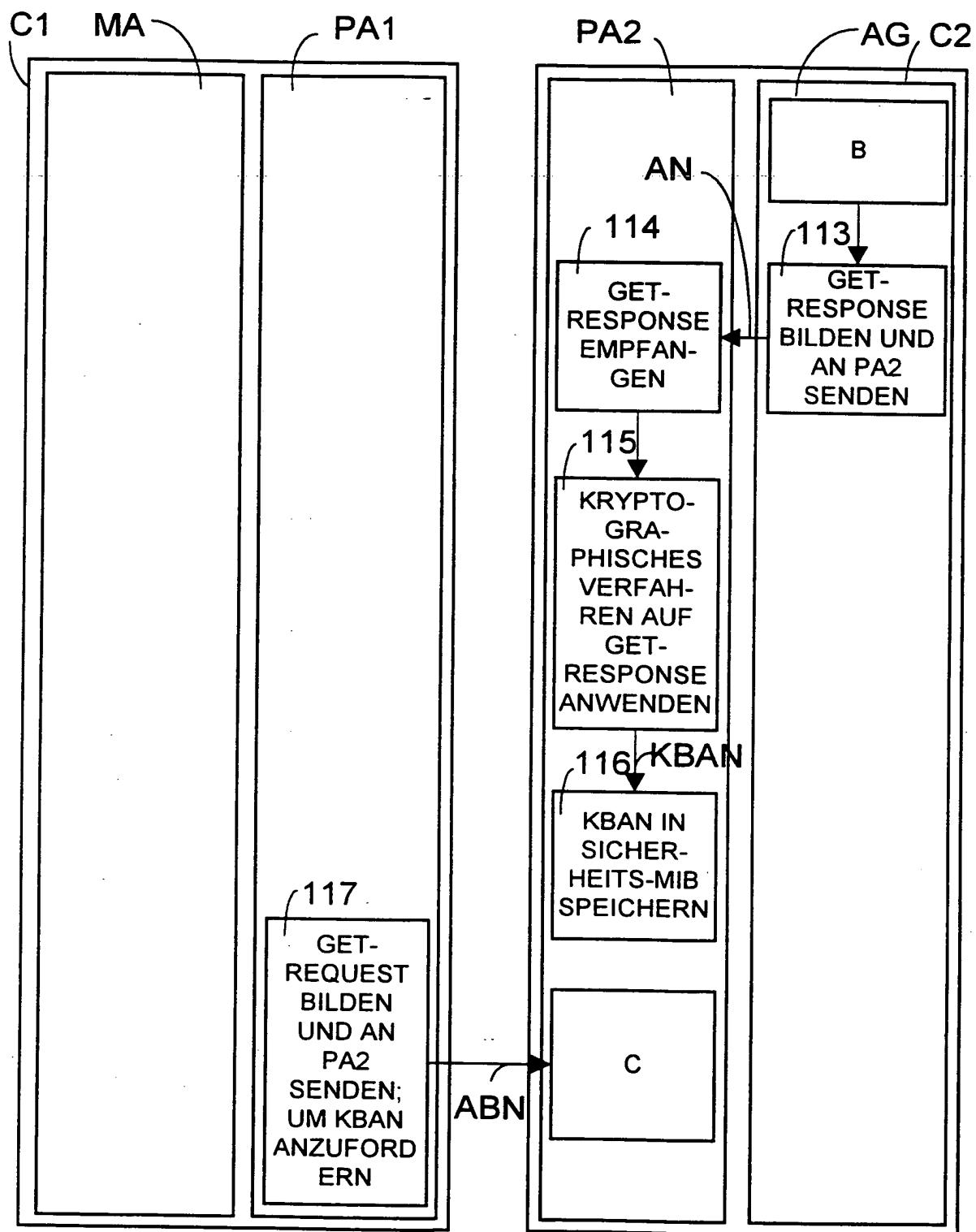
2/10

FIG 1



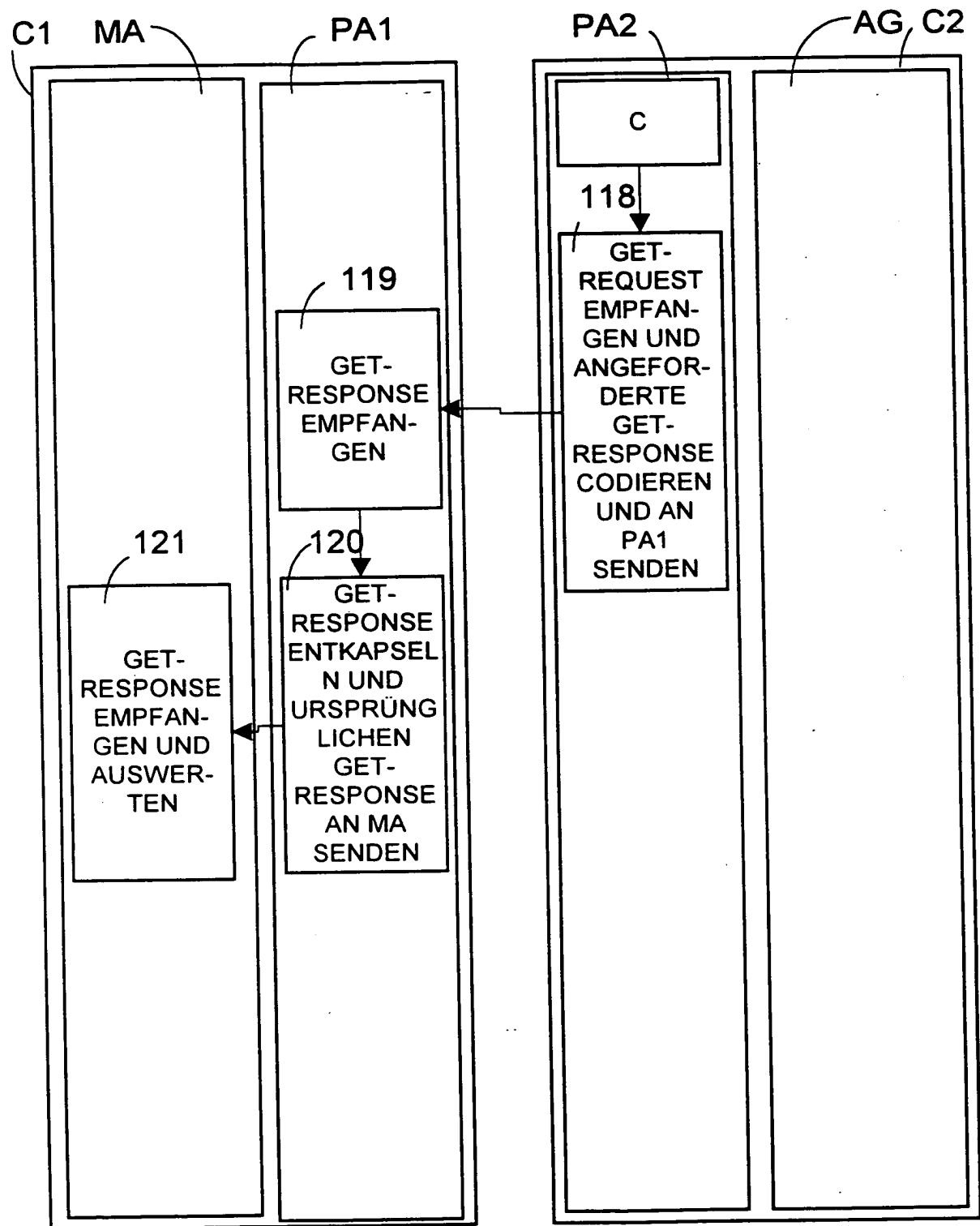
3/10

FIG 1



4/10

FIG 1



5/10

FIG 2

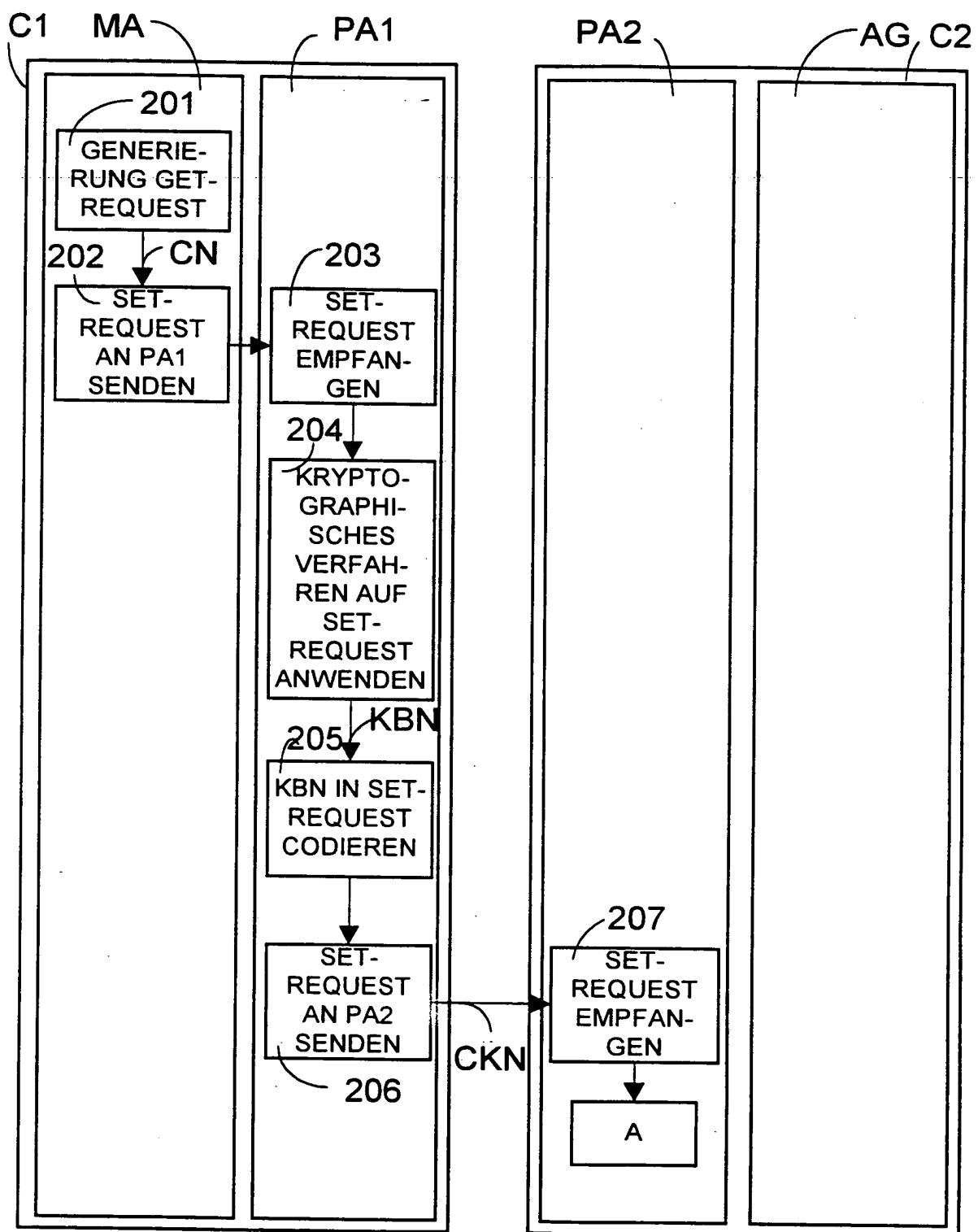
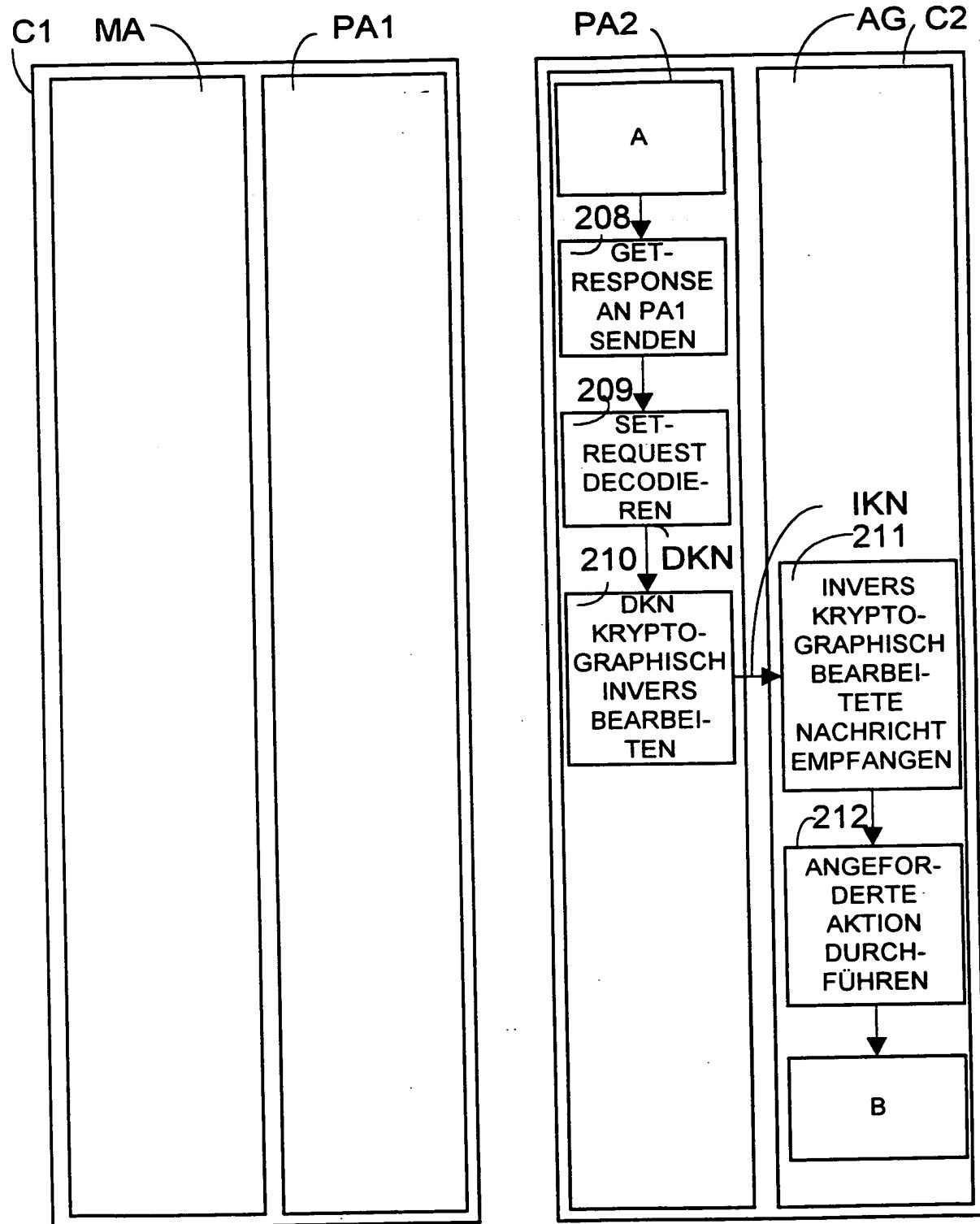
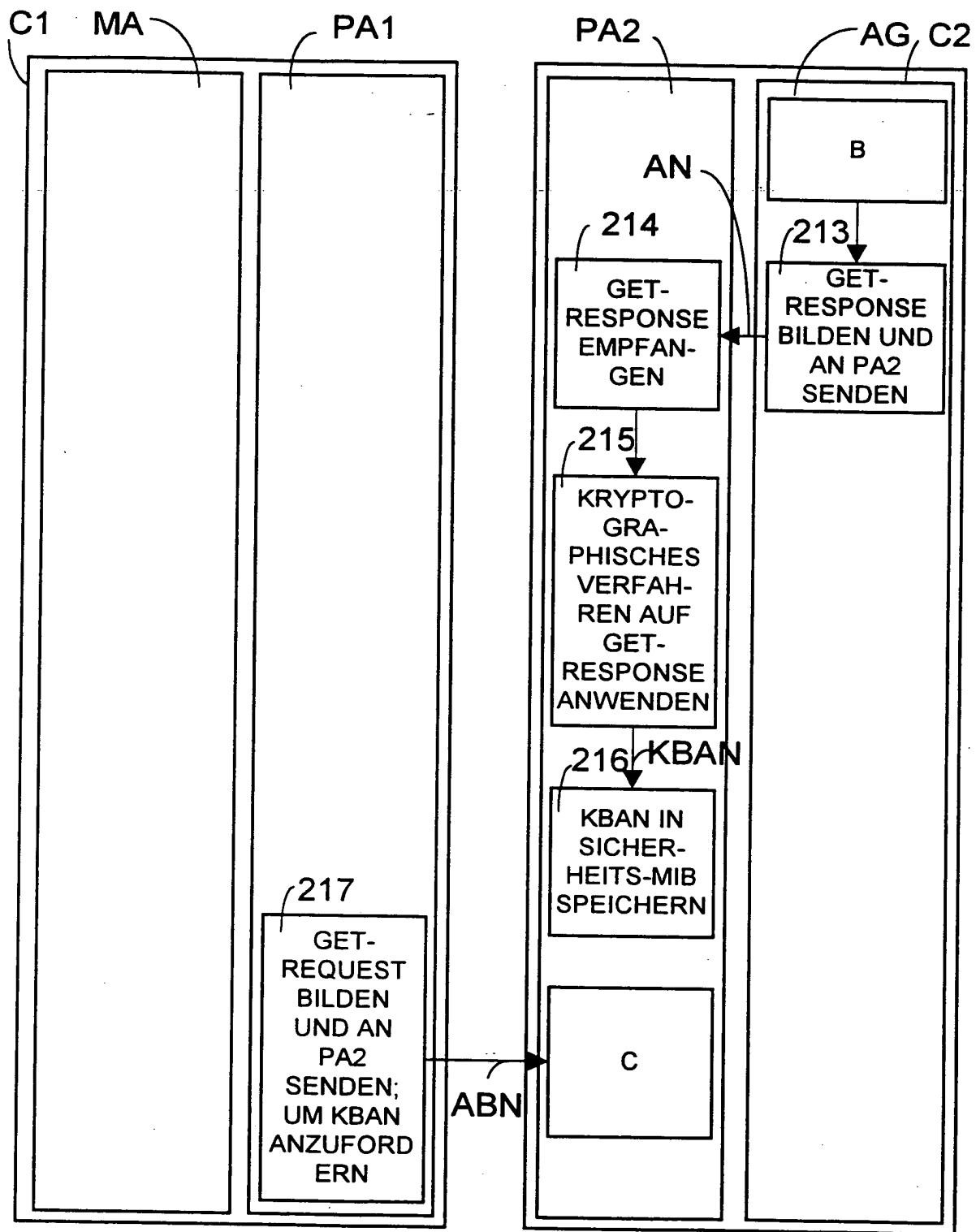


FIG 2



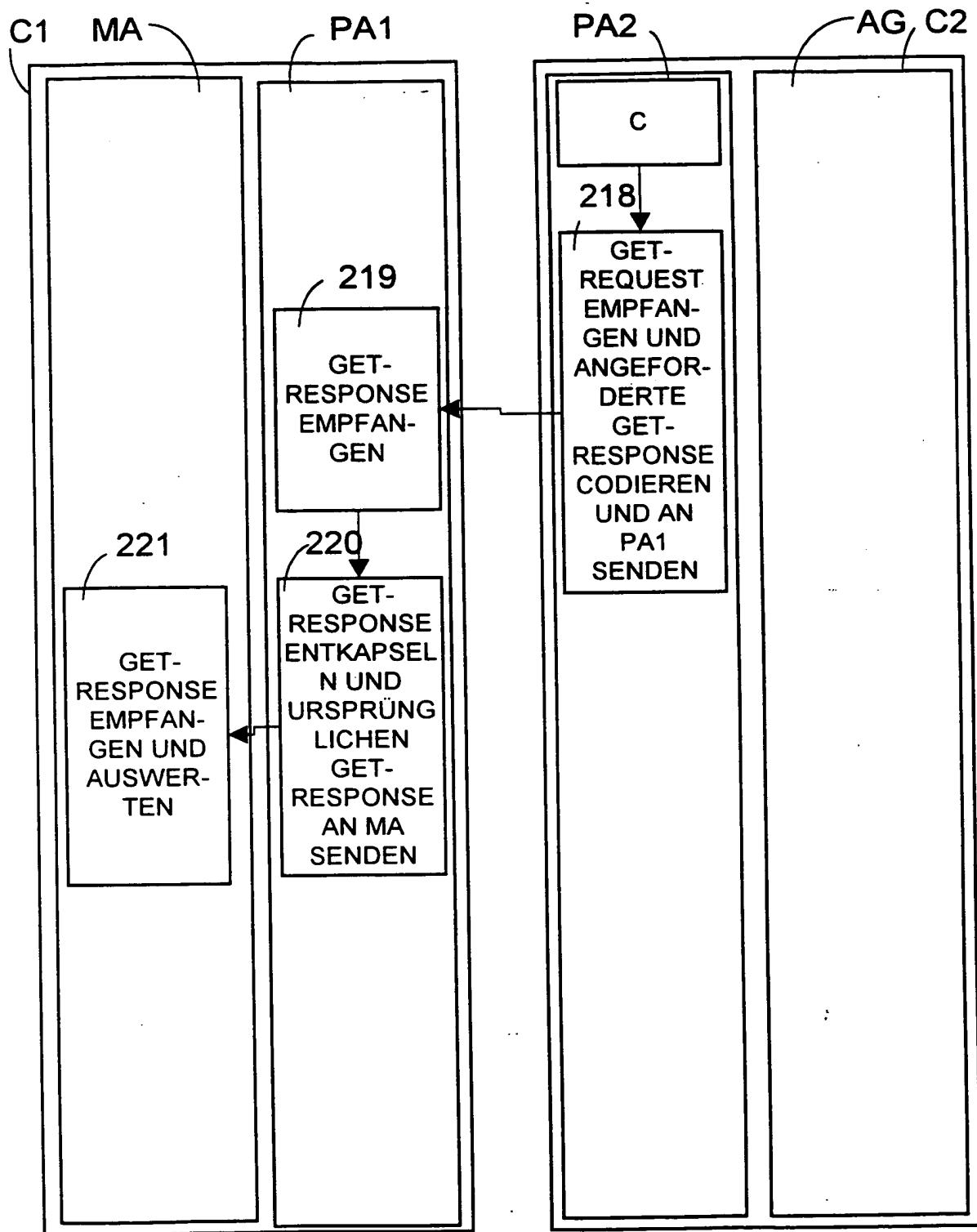
7/10

FIG 2



8/10

FIG 2



9/10

FIG 3

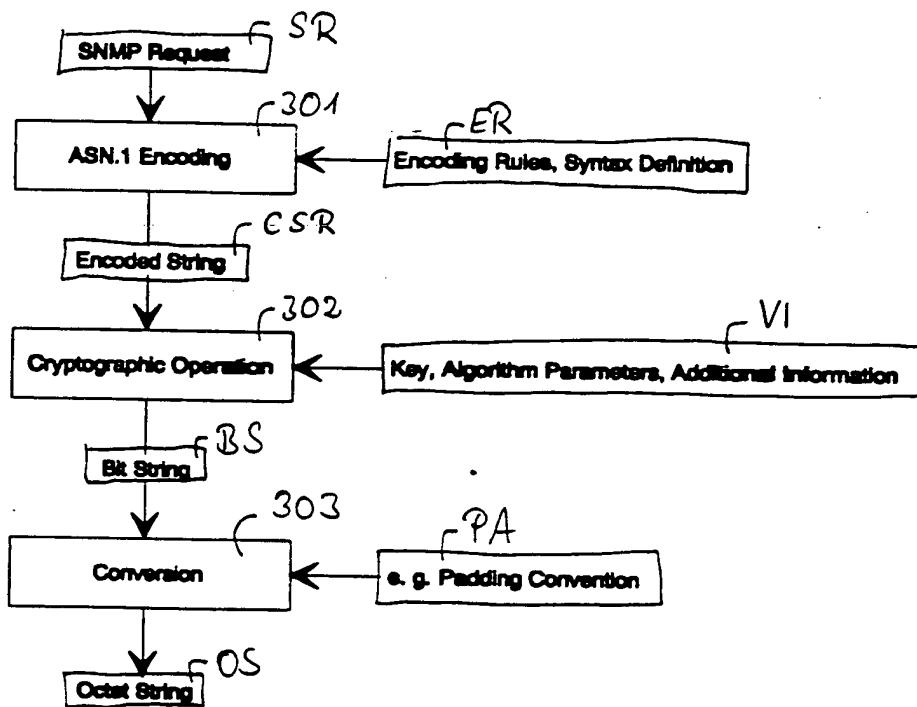
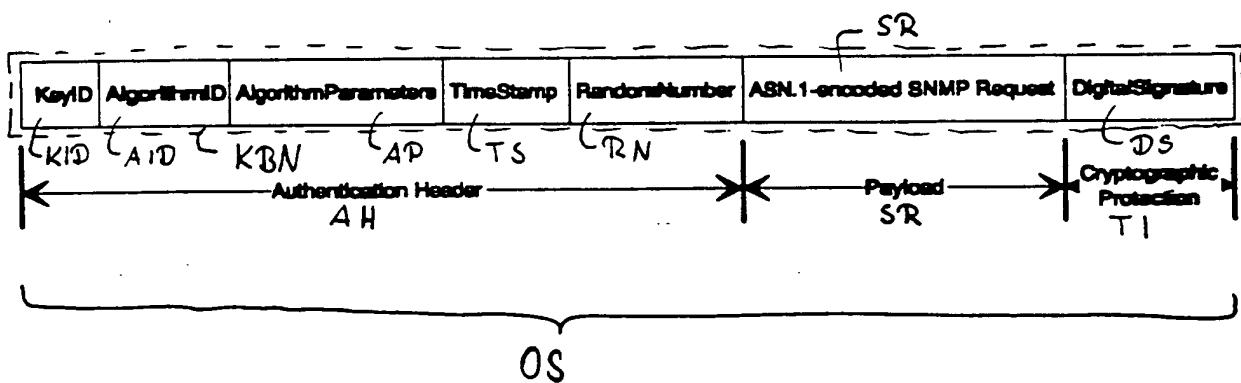


FIG 4



10/10

FIG 5

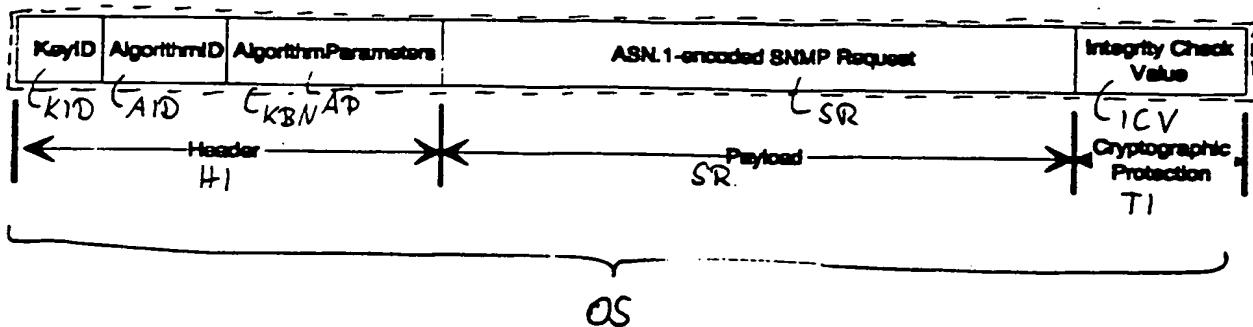
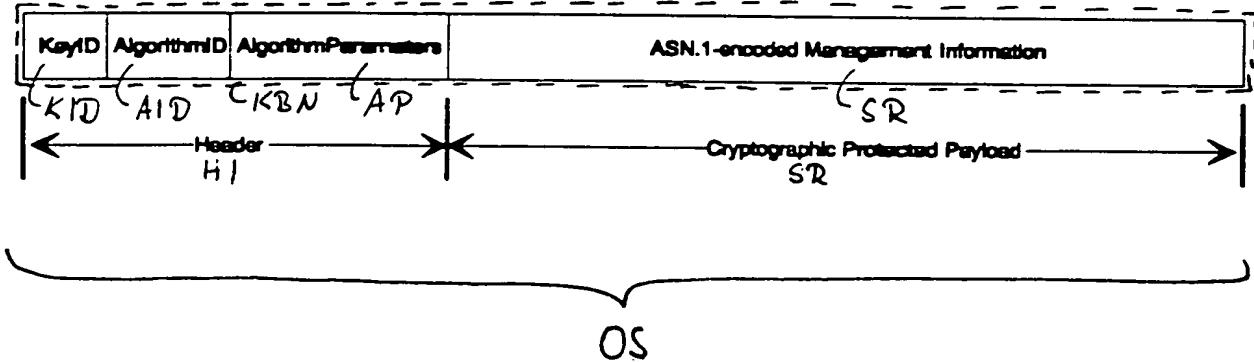


FIG 6



This Page Blank (uspto)